

REMARKS

Reconsideration of the application in light of the above amendments and the following remarks is respectfully requested.

Status of the Claims

Claims 5-15 are pending. Claims 1-2 were cancelled in a previous amendment. Claims 3-4 have been withdrawn from consideration.

Claims 5, 7-8, and 13-15 have been amended. New claims 16-18 have been added. Support for the amendments to claims 5, 7-8, and 13-15, and for new claims 16-18, can be found, for example, in the Specification on page 5, paragraphs 0018-0019, and page 6, paragraph 0024-0026.

No new matter has been added.

Amendments to the Specification

Applicants have amended the Specification to fix a minor typographical inaccuracy. No new matter has been entered.

Objection to the Claims

The Examiner has objected to claims 13 and 14 for containing informalities. Applicants have amended claims 13 and 14 and submit that claims 13 and 14 are in compliance. Applicants respectfully request reconsideration and withdrawal of the objection.

Rejection under 35 U.S.C. §101

Claims 5-14 were rejected under 35 U.S.C. §101 because the Examiner contends that the claimed invention is directed to non-statutory subject matter. Applicants respectfully traverse the rejection.

In response to Applicant's November 10, 2006 Amendment, the Examiner acknowledges that using a key for transmitting messages is a concrete, tangible, and useful result. *See*, Detailed Action, Item 2, Page 3, paragraph 1. However, the Examiner contends that "although the key can be used for transmitting messages . . . the claim does not set forth any steps in which a transmission of a message actually occurs." (Detailed Action, Item 2, Page 3, first paragraph, lines 1-4.) Applicants respectfully disagree.

Applicants respectfully note that claims 5, 7, and 13 each recite the steps of generating a message, sending the message, encrypting the received message, and then sending the encrypted message to a set of recipients. Therefore, since the claims 5, 7, and 13 each actively recite steps of sending messages, Applicants respectfully submit that the sending of messages constitutes a "transmission of a message."

Notwithstanding the above remarks, Applicants have amended independent claims 5, 7, and 13 to recite the steps of encrypting, and transmitting the encrypted message which has been encrypted using the common key k . Claims 5, 7, and 13 now actively recite features of encrypting and sending an encrypted message, which Applicants respectfully submit is a concrete, tangible, and useful result, and therefore, constitutes statutory subject matter. *See*, Detailed Action, Item 2, page 3, paragraph 2.

Claim 6 depends from claim 5. Claims 8-12 depend from claim 7. Claim 14 depends from claim 13. Applicants submit that claims 6, 8-12, and 14 are also directed to statutory subject matter based on their respective base claim.

Reconsideration and withdrawal of the rejection of claims 5-14 under 35 U.S.C. §101 is respectfully requested.

Rejection Under 35 U.S.C. § 112, second paragraph

Claims 5-15 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Applicants respectfully traverse the rejection.

With respect to the Examiner's contention that "it appears that the claim does, in fact, require direct access to the random number $z1$ " (*see*, Detailed Action, Item 2, page 3, paragraph 3, lines 5-9., and Item 9, page 7, paragraph 2, lines 1-7), Applicants respectfully disagree. As discussed in Applicants November 10th Response, each subscriber T_j ($j \neq 1$) is provided with access to the random number $z1$ **in encrypted form**. In particular, each subscriber T_j ($j \neq 1$) receives the encrypted random number $z1$ via message M_{1j} . Claim 5 recites the step of "sending, by the first subscriber $T1$, the random number $z1$ to all other subscribers T_j , $j \neq 1$, **in encrypted form** by generating a message M_{1j} ." This feature is similarly recited in claim 7, lines 10-12, and in claim 13, lines 12-14. As will be discussed below, since each subscriber T_j , $j \neq 1$ receives k^{1j} , and also possesses k^{j1} , each subscriber T_j , $j \neq 1$ can decrypt the encrypted random number $z1$. Therefore it is not necessary to provide each subscriber T_j , $j \neq 1$ with "direct access" to the random number $z1$.

With respect to the Examiner's contention that "it is not clear how each subscriber T_j ($j \neq 1$) has access to the transmission key k^{1j} " (*see*, Detailed Action, Item 2, page 3, paragraph 3, line 9 through page 4, paragraph 1, line 7, and Item 9, page 7, paragraph 2, line 7 through page 8, paragraph 2, line 2), Applicants respectfully note that claims 5, 7, and 13 also recite that the message M_{1j} is encrypted using $E(k^{1j}, z1)$, which is **symmetrical** encryption algorithm. It would be apparent to one of ordinary skill in the art that a symmetrical encryption algorithm indicates that symmetrical keys are used — *i.e.*, $k^{1j} = k^{j1}$. Therefore, contrary to the Examiner's position,

Applicants submit that the properties of the transmission key k^{1j} are indeed recited in claims 5, 7, and 13.

Notwithstanding the above remarks, Applicants have amended claims 5, 17, and 13 to recite that each subscriber T_j , $j \neq 1$, computes the symmetrical counterpart of k^{1j} , *i.e.*, k^{j1} . Since each subscriber T_j , $j \neq 1$ possesses k^{1j} and k^{j1} , each subscriber T_j , $j \neq 1$ can decrypt the encrypted random number $z1$.

Further, regarding the Examiner's contention that the variable " k^{j1} " is not defined in claims 5 and 6, (*see*, Detailed Action, Item 2, page 4, Paragraph 3 through page 5, paragraph 1, and in Item 9, page 9, paragraph 4), Applicants respectfully disagree. Claim 6 recites inherent properties of the symmetrical encryption algorithm recited in claim 5. Applicants respectfully submit that since symmetrical keys are used, Applicants have, by definition, defined the variable " k^{j1} " in that " k^{j1} " is inherently equal to the " k^{1j} " recited in claim 5. Claim 11 recites inherent properties of the symmetrical encryption algorithm recited in claim 7, in the same manner as discussed above. Notwithstanding the above remarks, as Applicants have amended independent claims 5 and 7 to recite that k^{j1} is a symmetrical counterpart of k^{1j} , Applicants note that this point of rejection is moot with respect to claims 6 and 11.

With respect to the Examiner's contentions regarding insufficient antecedent basis for the features of "the respective first message," "the received respective first message N_j ," "the transmission key k^{1j} ," and "the encrypted second message $M1j$ " recited in claims 7 and 13, (*see*, Detailed Action, Item 9, page 9, paragraph 2 and page 10, paragraph 2), Applicants respectfully disagree. Contrary to the Examiner's position, claims 7 and 13 recite "a respective first message N_j " (claim 7, line 5; claim 13, line 6) which is "the respective first message" sent by each of the

subscribers T_j , $j \neq 1$ (claim 7, line 7; claim 13, line 8). The sent respective first message is the message on which the first subscriber T_1 computes a transmission key k^{1j} (claim 7, lines 8-9; claim 13, lines 10-11). Further, claims 7 and 13 both recite “computing a transmission key k^{1j} ” (claim 7, line 8; claim 13, line 10) which is used to during the encrypting of the second message M_{1j} (claim 7, lines 10-12; claim 13, 12-14). Notwithstanding the above remarks, Applicants have amended claim 7 and 13 to include the appropriate variable name where appropriate so as to avoid confusion.

With respect to the Examiner’s contentions regarding the features of “the respective random number z_j ” recited in claim 8 (*see*, Detailed Action, page 9, paragraph 3), Applicants have amended claim 8 to recite that “each respective random number z_j is selected from the set.”

With respect to the Examiner’s contentions regarding the logical consistency and clarity of the claims (*see*, Detailed Action, Item 2, page 4, paragraph 1; Item 9, page 7, paragraph 2 through page 8, paragraph 1; Item 9, page 8, paragraph 3 through page 9, paragraph 1; and Item 9, page 9, paragraph 5 through page 10, paragraph 1), Applicants respectfully note the following.

As discussed above, Applicants respectfully note that in the method recited in claims 5, 7, and 13, it is not necessary for each subscriber T_j , $j \neq 1$, to have direct access to the random number z_1 . As recited in the claim, each subscriber generates a respective message N_j , which is based on a respective random number z_j . Then, each subscriber T_j transmits its respective message N_j to each of the other subscribers T_j (except for itself), as recited in claims 5 (lines 7-8), 7 (lines 7-8), and 13 (lines 8-9). After receiving the messages N_j from each of the other subscribers T_j , the first subscriber T_1 creates a respective transmission key k^{1j} for each of the subscribers T_j , $j \neq 1$, as recited in claims 5 (lines 10-12), 7 (lines 9-10), 13 (lines 11-12). The first subscriber T_1 then sends the

encrypted random number $z1$ to all the other subscribers T_j , $j \neq 1$, by generating a message M_{1j} (lines 15-18 in claim 5; lines 13-15 in claim 7; lines 15-17 in claim 13).

As noted above, the message M_{1j} is created using "a symmetrical encryption algorithm in which the random number $z1$ is encrypted with the transmission key k^{1j} ." Thus, when each subscriber T_j , $j \neq 1$, receives the message M_{1j} which contains the encrypted random number $z1$, the respective subscriber T_j , $j \neq 1$, is able to decrypt the encrypted random number $z1$ because $k^{1j} = k^{j1}$. More specifically, Applicants respectfully note the following properties of $k^{1j} = k^{j1}$:

- $N^j = g^{zj} \bmod p$: see line 4 of claim 5; line 5 of claim 7, and line 6 of claim 13
- $k_{12} = N_1^{z2} \bmod p$: see lines 10-12 of claim 5, lines 9-10 of claim 7, and lines 11-12 of claim 13.
- By simple substitution: $k_{12} = N_1^{z2} \bmod p = ((g^{z1}) \bmod p)^{z2}$
- Using the properties of exponentials: $k_{12} = N_1^{z2} \bmod p = ((g^{z1}) \bmod p)^{z2} = g^{(z1 * z2)} \bmod p$
- Using the properties of exponentials: $k_{12} = N_1^{z2} \bmod p = ((g^{z1}) \bmod p)^{z2} = g^{(z1 * z2)} \bmod p = (g^{z2} \bmod p)^{z1}$
- By simple substitution (recall that $k_{21} = N_2^{z1} \bmod p$): $k_{12} = N_1^{z2} \bmod p = ((g^{z1}) \bmod p)^{z2} = g^{(z1 * z2)} \bmod p = (g^{z2} \bmod p)^{z1} = N_2^{z1} \bmod p = k_{21}$

Thus, as demonstrated above, $k_{12} = k_{21}$. Accordingly, since each subscriber T_j , $j \neq 1$, now has a symmetrical key for the message transmitted by T_1 , each subscriber T_j , $j \neq 1$, can now calculate the random number $z1$. *See*, Specification, page 5, paragraphs 0018, 0024. As a point of clarification, Applicants have amended independent claims 5, 7, and 13 to recite that each subscriber T_j , $j \neq 1$, computes the symmetrical counterpart k^{j1} of the transmission key k^{1j} .

Each subscriber T_j is then able to calculate a common key $k:=h(z_1, g^{z_2} \dots g^{z_n})$ because $h(x_1, x_2 \dots x_n)$ has the property that it is symmetrical in its arguments $x_2 \dots x_n$. *See*, Specification, paragraph 0026. Namely, at this point, each subscriber T_j has determined the value of the random number z_1 , as described above. Additionally, each subscriber T_j already possesses $N_2 = g^{z_2} \bmod p \dots N_n = g^{z_n} \bmod p$ because that information was already transmitted in the first two steps recited in claims 5 (lines 4-9), 7 (lines 5-8), and 13 (lines 6-9). Thus, each subscriber T_j has the information necessary to calculate the common key k based on the function h , as recited in claims 5, 7, and 13.

In view of the above remarks, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 5-15 under 35 U.S.C. §112, second paragraph.

New Claims

New claims 16-18 are directed to decrypting of the transmitted encrypted message by another subscriber which has received the transmitted encrypted message. It is respectfully submitted that new claims 16-18 constitute patentable subject matter.

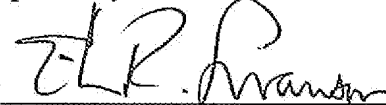
CONCLUSION

Each and every point raised in the Final Office Action mailed February 5, 2007, and the Advisory Action mailed April 13, 2007, has been addressed on the basis of the above remarks. In view of the foregoing it is believed that claims 5-18 are in condition for allowance and it is respectfully requested that the application be reconsidered and that all pending claims be allowed and the case passed to issue.

If there are any other issues remaining which the Examiner believes could be resolved through a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at the telephone number indicated below.

Dated: May 2, 2007

Respectfully submitted,

By 

Erik R. Swanson
Registration No.: 40,833
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant